OneLondon Data Sharing Framework

Approval Body	London Information Governance Steering Group
Version	0.6
Issue Date	08/03/2021

Version	Summary of Changes	Date
0.6	Revisions following initial stakeholder consultation with STP/ICS and local IG groups and forums. Including London SIGNs Forum	08/03/2021
0.5	Revisions following OneLondon IG Leads review and commentary	09/12/2020
0.4	Final Internal Review	11/11/2020
0.4	Revisions following OneLondon IG Leads review and commentary	06/11/2020
0.3	Final Internal Review	25/09/2020
0.2	Revisions following OneLondon IG Leads review and commentary	22/09/2020
0.1	First draft	27/07/2020

1. Introduction

1.1. OneLondon started out as a Local Health and Care Record Exemplar (LHCRE), transitioning to a sustainable component of London's regional landscape at the end of March 2021. OneLondon is a programme designed, planned and managed by a partnership of health and care organisations, working together with the London population and London's health and care providers, to join up personal data to support fast, effective, and safe care delivery through better integration of care, reduction of service user risks and better planning of services.

1.2. This is achieved by connecting health and care records across London enabling near real-time data sharing amongst health and care organisations; supporting the clinical health activities concerned with the prevention, investigation, and treatment of illness and improving both patient and service user experience.

1.3. The OneLondon programme will also support health and care planning, service improvement, system development and translational research.

1.4. This OneLondon Data Sharing Framework is a high-level description of the principles for data sharing in London. It represents what is happening at a Sustainability and Transformation Partnership/Integrated Care System (STP/ICS) level and provides a direction of travel to ensure that local STP/ICS frameworks are aligned with each other.

1.5. The Data Sharing Framework sets out the jointly agreed principles to support interoperability, including but not limited to audit, opt-out, roles-based access (RBAC), and sensitive data items.

1.6. The OneLondon Data Sharing Framework aims to:

- Provide a memorandum of understanding between London's STPs/ICSs as to how they will work together
- Provide reassurance to the system and stakeholders that STPs/ICSs are progressing in one direction with regards to data protection

1.7. The Data Sharing Framework should act as a reference for data controllers and data processors across London's health and care system (including, but not limited to, information governance and health and care professionals). The framework will be

supported by public-facing materials to describe its purpose and how it will be delivered.

2. OneLondon Programme Structure

2.1. OneLondon and the ICSs are not legal entities and are not data controllers or data processors. Nor are they granted delegated data controller responsibility.

2.2. The individual ICSs are partnerships that bring together providers and commissioners of NHS services across a geographical area together with local authorities and other local partners. These organisations are the data controllers. They agree to share the data of those that they provide health and care services to. Each ICS Information Governance (IG) Lead is responsible for taking any recommendations back to their local data controllers for appropriate sign-off.

2.3. These data controllers agree, by mutual arrangement (i.e. ICS arrangement), the means and purposes of processing personal data within their geographical boundaries. Where data is shared across a wider geographical footprint, i.e. beyond London, ICSs are responsible for these data sharing arrangements locally. These arrangements should be consistent with the principles of this OneLondon Data Sharing Framework.

2.4. Each ICS is a collective representation of the health and care providers (i.e. data controllers) which are party to the ICS level arrangement within a geographical boundary. These are:

- North West London
- North East London (East London Health and Care Partnership)
- North Central London (North London Partners in Health and Care)
- South East London (Our Healthier South East London)
- South West London Health and Care Partnership

2.5. The data controllers in each ICS will engage with OneLondon through their own individual ICS governance structure. Each ICS is responsible for ensuring that they have an IG group that meets to discuss local and OneLondon issues.

2.6. Each ICS will have an appointed representative on the London Information Governance Steering Group (LIGSG) representing the views of their local providers. The appointee will provide communication between OneLondon and ICSs and vice versa (information, updates, feedback, etc.), and must therefore be given sufficient time to consult with local data controllers as necessary.

3. Background to OneLondon Data Sharing Framework

3.1. The Data Sharing Framework is a non-commercial and non-legally binding statement of cross-ICS data sharing principles that are predicated in data protection legislation and the common law.

3.2. Health and care providers have a duty to share information for the purposes of health and care where it is likely to facilitate the provision to the individual of health services or adult social care in England, and in the individual's best interests.

3.3. This must be undertaken in the best interests of their patients/service users and within the framework set out by the data protection legislation, Common Law Duty of

Confidentiality, Caldicott Principles, and the Information Commissioner's Office Data Sharing Code of Practice.

3.4. This Data Sharing Framework summarises the legal principles and good practice guidelines placed on health and care providers within the five London ICSs for wider data sharing.

4. Purpose of the OneLondon Data Sharing Framework

4.1. The purpose of the OneLondon Data Sharing Framework is to support improved health and care delivery across the London region. As such it sets out the jointly agreed principles to support interoperability, including but not limited to audit, opt-out, role-based access (RBAC), and sensitive data items.

4.2. As an initial phase, as part of the OneLondon programme, this purpose is being achieved through a number of interoperability projects being pursued by the individual ICSs.

4.3. These projects shall include but not be exclusive to:

- **Health Information Exchange** – Ubiquitous data viewing by the clinician at the point of care across a range of settings through an integrated Health Information Exchange hub model.
- **Longitudinal Care Record** – Normalised longitudinal care record to support the full range of direct care, population health management, clinical improvement, analytics, and research.
- **Personal Health Record** – Patient/service user self-access to their health and care record.
- **Data Services Layer** – This provides a data service that supports population health, direct care applications, and other care systems with appropriate controls and publish and subscribe mechanisms.
- **Use of de-identified data for Service Improvement and Planning** – To develop London-wide governance of trusted local clinical improvement methodology.
- **Use of de-identified data for Research** – To provide a data approach for translational and transformational research regionally, nationally and beyond.

4.4. Data sharing mechanisms support the above initial projects at the ICS level between the respective health and care data controllers.

4.5. Each ICS has implemented data sharing arrangements between its respective data controllers with appropriate DPIAs and data processing agreements. These shall entail reference being made within ICS data sharing arrangements to the OneLondon programme as a use-case for data sharing where relevant.

4.6. Each individual data controller is responsible for the provision of:

- DPIA; and
- Privacy notices.
- Lawful arrangements for the sharing of personal information and aggregate information.

4.7. Data controllers within each ICS are responsible for the quality and coverage of the materials that articulate the sharing of data as part of the OneLondon initiative.

4.8. Data controllers are responsible for discharging their obligations that are assured through the Data Security and Protection Toolkit and compliance with all NHS and legal obligations and requirements. These assurance processes are monitored via individual ICS arrangements.

4.9. Any new, changed or de-listed data controller is managed within the appropriate ICS in line with the jointly agreed principles set out in this Data Sharing Framework.

4.10. ICS arrangements determine the geographical scope for data sharing under the OneLondon Data Sharing Framework.

5. Participation to the OneLondon Programme

5.1. ICSs participating in the sharing of personal data for the purposes of the OneLondon programme are responsible for uploading relevant documentation to the Data Controllers Console (the 'DCC'). This is the platform for health and care organisations in London to store, update and track the status of data sharing.

5.2. The documents which are required to be uploaded on to the DCC include any relevant data processing agreement(s) and data sharing use-case(s) including, the data controllers party to a data sharing use-case within the ICS.

6. Access and control

6.1. This Framework describes a joint agreement between ICS partners to the implementation of appropriate access controls by the data controllers. More detailed requirements shall be subject to LIGSG approval routes.

6.2. This Framework describes a joint agreement between ICS partners for privacy monitoring arrangements to ensure the appropriate implementation of access controls and to interrogate accesses to systems. More detailed requirements shall be subject to LIGSG approval routes.

6.3. All data controllers shall utilise role-based access controls (RBAC) to access any OneLondon system. The RBAC must comply with NHS Digital RBAC standards.

7. Use of fully de-identified data for planning and translational research

7.1. This Framework describes a joint agreement between ICS partners to the implementation of appropriate controls on the use of fully de-identified data for planning and translational research in a manner consistent with the National Data Opt Out:

- Each request to access de-identified data is documented and reviewed by an appropriate multidisciplinary data access group to ensure that there is compliance with data protection legislation and supports healthcare knowledge and improvement.
- The data will be accessed in an environment that is secure, accredited, monitored and prevents unauthorised use.
- There is no syndication, extraction, or transfer of data without appropriate data sharing and/or data processing agreements that fully articulate legal responsibilities.
- Data is not sold (this includes gifts given in lieu).

APPENDICES

Appendix I. Examples of data to be shared

The following table sets out summary examples of the data to be shared across all of the interoperability objectives to facilitate the OneLondon initiative with appropriate de-identification controls[1] where data is to be used for non-direct care / secondary purposes.

Data Subjects	**Patients / service users treated in London by an NHS Provider**
Type of Data	Personal Data and healthcare data
Example of Data Categories	Demographic data: Name; Address; Postcode; Date of Birth; Age; Sex; Contact Details; Physical Description' NHS Number (consistent identifier); Next of Kin details
Special Category Data	All health data except where restricted by Statute; Ethnicity; genetic information; or where a patient/service user has requested restriction, e.g. Transgender
Volume	All relevant health data except where restricted by Statute to be made available.
Frequency	Real-time/near real-time calling of data from local NHS Provider systems by requesting NHS provider at point of care.

Appendix II. Lawful Basis for Data Sharing

1. Introduction

1.1. The sharing and processing of personal data and special category data, as part of the data processing, is regulated by the Data Protection Act 2018 and other applicable legislation.

1.2. Personal Data is shared and processed for the purposes of the OneLondon programme in accordance with the principles relating to processing under Article 5 GDPR, and where a clear lawful basis is set out under Articles 6 and 9 GDPR for personal data and special category data, respectively.

1.3. The rules for data processing amongst NHS Health and Social Care Providers are:

Article 6(1) UK GDPR	**Article 9(2) UK GDPR (and Schedule 1 to the Data Protection Act 2018**
(c) The processing is necessary to comply with legal obligations	(c) The processing is necessary to protect the vital interests of the data subject or of another natural person where the data subject is physically or legally incapable of giving consent.

[1] In accordance with the ICO's Anonymisation: managing data protection risk code of practice

(d) The processing is necessary to protect the vital interests of the data subject or another person	(g) the processing is necessary for reasons of substantial public interest, on the basis of UK or EU law (*for instance, the discharge of statutory functions)*
(e) The processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the data controller	(h) processing is necessary for the purposes of preventive or occupational medicine, for the assessment of the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or the management of health or social care systems and services (*in accordance with Schedule 1 paragraph 2 to the Data Protection Act 2018).*
	(i) processing is necessary for reasons of public interest in the area of public health, including ensuring high standards of quality and safety of healthcare *(in accordance with Schedule 1 paragraphs 2 and 3 to the Data Protection Act 2018)*.
	(j) processing is necessary for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1) based on Union or Member State law which shall be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject.

2. The Health and Social Care Act 2012 (as amended by the Health and Social Care (Safety and Quality) Act 2015)

2.1. Health and Care Providers are supported by s. 251B of the Health and Social Care Act (as amended by the Health and Social Care (Safety and Quality) Act 2015) to share personal data where it facilitates health and/or social care for an individual and is in the individual's best interests. However, this legal basis for disclosure can only be relied upon in the above two circumstances and on a case-by-case scenario.

2.2. The GDPR / Data Protection Act 2018, Article 9(2)(h) is the permissive legislation which allows for disclosure of information between relevant bodies in relation to relevant information, as opposed to the Health and Social Care (Safety and Quality) Act 2015 which states that health and care providers can disclose confidential information in respect of the two circumstances that are mentioned above.

3. Other Relevant Legislation

3.1. Further laws and regulations by which health and care providers are bound set out the supplementary requirements around the use of personal confidential data. These include, but are not limited to, legislative changes in relation to COVID-19, the NHS Act 2006, Health and Social Care Act 2012, the Human Rights Act 1998, the Common Law Duty of Confidentiality. Health and Care providers are bound by the Access to Health Records Act 1990 as regards the sharing and processing of deceased patient / service user's data.

4. Common Law Duty of Confidentiality

4.1. The dissemination and sharing of confidential information amongst health and care providers and their data processors is lawful and the common law duty of confidence is discharged where there is a statutory provision permitting such disclosure. The UK GDPR sets out in Article 9(2)(h), assuming Article 6 is complied with, that processing is permitted where it is necessary for the purposes of preventive or occupational medicine, for the assessment of the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or the management of health or social care systems and services.

4.2. Data sharing under the OneLondon Framework is considered to fall within the reasonable expectation of the data subjects insofar as this is sharing to support direct care under the Health and Social Care (Safety and Quality) Act 2015. Public deliberation in the use of health and care data has been undertaken in support of OneLondon to support the commitment to respecting the reasonable expectations of patients/service users.

5. Data Protection Arrangements

5.1. Each individual data controller has a legal duty to uphold the rights and freedoms of data subjects.

5.2. Each data controller is responsible for the management of subject access requests and upholding all data subjects' rights. Data controllers have a responsibility to coordinate with relevant data processors.

5.3. As part of this Data Sharing Framework, ICS partners commit to appropriate transparency arrangements in line with their current local ICS arrangements.

5.4. ICS-based digital projects will be subject to data controller-led Data Protection Impact Assessments (DPIAs) and transparency requirements coordinated at ICS governance groups. Where data flows between ICS partners across London and between ICSs, data controllers may agree to subject proposals to a joint shared DPIA.

Management of Data Subjects' Rights

6. Right to be informed

6.1. Each data controller shall ensure patients and service users are informed of the processing and sharing of their data and the rights that they have in relation to this.

6.2. This requires data controllers to publish appropriate fair processing information (typically via a privacy notice) which includes reference to data sharing for the purposes of health and care provision.

6.3. Each data controller shall be responsible for the provision of their own privacy notices in accordance with the ICO guidance on privacy notices and the DSP Toolkit.

7. Right of Access

7.1. Patients and service users have the right to obtain access to their personal data.

7.2. The OneLondon programme is not a data controller, nor is an ICS. As such, any subject access request made by a patient/service user must be directed to a data controller.

7.3. The data controller in receipt of the subject access request is required first to check whether any personal data of the person seeking information is being processed.

7.4. The Longitudinal Health and Care Record should be accessible to all data controllers within each ICS, dependent on use and access controls.

7.5. Where a subject access request is made to a data controller that does not hold a legitimate relationship with the patient/service user, there will be nothing to disclose.

7.6. Each individual data controller is responsible for communicating directly with any individual undertaking a subject access request unless the data being requested falls outside of data controllership / joint data controllership.

7.7. Where data is being processed, the data controller is required to discharge the subject access request whilst observing the provisions of the DPA 2018 / GDPR.

7.8. This requires all subject access requests to be discharged by the data controllers as per the law. Health and care organisations are required by the DSP Toolkit to maintain metrics of subject access request response performance and compliance.

8. Right to Rectification

8.1. Patients/service users are entitled to have their personal data rectified if it is factually inaccurate or incomplete. However, where clinical information is challenged as being inaccurate or incomplete, the decision to rectify this must be clinically-led by the relevant treating consultant. In these instances, a note of question / issue raised will be recorded against the relevant details.

8.2. In practical terms, data controllers receiving rectification requests must ensure that the data controller responsible for the source system is made aware of, and implements, the rectification request whilst observing the provisions of the DPA 2018 / GDPR. This includes taking clinical responsibility for the accuracy of data and any decision to rectify a record. This process will be managed in place with current local arrangements.

9. Right to Erasure

9.1. Patients/service users are entitled to have their personal data erased at their request in a limited number of circumstances. However health and care providers will not

'erase' personal data where that processing is necessary for reasons of public interest in the areas of provision of healthcare, public health, and/or scientific research.

9.2. Where the erasure request covers data from a source system of another joint data controller, the request must be lodged with the source data controllers and monitored by the receiving data controller.

10. Right to Restrict Processing

10.1. Patients/service users have the right to compel organisations to continue to store personal data but not process it any further, at their request. However, health and care providers will not restrict the processing of personal data where that processing is necessary for reasons of public interest in the areas of provision of healthcare, public health, and/or scientific research.

10.2. It is the responsibility of the data controller to manage this within their local system and not as part of the shared care record.

11. Right to Object

11.1. Individuals have the right to object to: Processing based on legitimate interest or performance of a task in the public interest/exercise of official authority; direct marketing; and/or, processing for the purposes of scientific/historical research and statistics.

11.2. When an individual raises an objection, the receiving data controllers are obliged to provide a response. Where the objection covers data from a source system of another joint data controller, the request must be lodged with the source data controllers and monitored by the receiving data controller.

12. Right related to automated decision making and profiling

12.1. This right provides safeguards for individuals against the risk that a potentially damaging decision is taken without human intervention.

12.2. The OneLondon programme does not currently include any systems in which decision-making is made without human intervention.

13. The National Data Opt-Out

13.1. The National Data Opt-Out applies only to the secondary use of identifiable personal data (i.e. non-direct care purposes).

13.2. Each individual data controller providing or coordinating publicly funded healthcare in England is responsible for compliance with the National Data Opt-Out.

13.3. Data controllers within each individual ICS are responsible for ensuring the services and systems are compliant with the National Data Opt-Out in their commissioning and designing of care systems.

13.4. The National Data Opt-Out does not apply to information that is anonymised in line with the ICO Code of Practice on Anonymisation or is aggregate or count-type data.

14. Freedom of Information Requests

14.1. Public authorities are individually responsible for discharging their legal responsibilities under the Freedom of Information Act (FOIA) 2000.

14.2. The OneLondon programme and local ICSs are not legal entities currently. Therefore, the individual public authorities (data controllers) are responsible for discharging freedom of information requests.

15. Fair Processing and Transparency

15.1. Schedules 2-4 Data Protection Act 2018 set out the requirement for data controllers to provide fair processing information to the patient/service user as regards how personal data is used.

15.2. Fair processing information should be delivered through privacy notices for each category of patient/service user about whom data is processed or shared.

15.3. Each data controller is individually responsible for publishing their own privacy information and is individually accountable for meeting these requirements as set out in Schedules 2-4 Data Protection Act 2018.

15.4. Arrangements at an ICS level may support the means by which the individual data controllers ensure the provision of fair processing and transparency materials to patients/service users. The OneLondon Data Sharing Framework does not modify ICS arrangements.

16. Technical and Organisational Standards

16.1. These are obligations placed on each data controller irrespective of their participation within an ICS or the OneLondon programme:

16.2. **ICO Registration:** All data controllers and data processors of personal data shall ensure and maintain registration with the Information Commissioner's Office (ICO) under the Data Protection Act 2018, and any registration requirements under subsequent legislation.

16.3. **NHS Digital Data Security and Protection Toolkit (DSP Toolkit):** All organisations which have access to health and care patient / service user data and systems are required by contract / NHS Digital to provide assurance, through an audited DSP Toolkit return lodged against their individual organisational code. This also includes the evidence requirement of achieving the required annual mandatory data security and protection staff training standard or an agreed action plan.

16.4. **Security of Processing:** Data controllers are obliged under the Data Protection Act, Section 56 to ensure that they implement appropriate technical and organisational controls to ensure an appropriate level of security in the control and processing of data. The security of processing is assured through independent audit of the DSP Toolkit return and compliance with the NHS Digital mandated standards relating to the NIS Directive, Cyber Essentials Plus and other related standards.